COUNTY OF LOS ANGELES
CHIEF INFORMATION OFFICE
500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

February 28, 2006

To: Supervisor Michael D. Antonovich, Mayor
Supervisor Zev Yaroslavsky, Chair Pro Tem
Supervisor Gloria Molina
Supervisor Yvonne B. Burke
Supervisor Don Knabe

From: Jon W. Fullinwider
Chief Information Officer

INFORMATION SECURITY STATUS FOR THE COUNTY OF LOS ANGELES

The attached document reflects the current status of information security for the County of Los Angeles along with a list of accomplishments over the past three years. Appendix A indicates the level of compliance to security best practices questions that were required for the last Business Automation Plan (BAP) submission. A similar set of questions have been included in the BAP instructions for this year to measure the amount of progress made by each department to implement identified security practices.

In the coming year, my office will submit update reports that will reflect changes in the County's security readiness and improvements achieved.

Please direct any questions regarding this report to Al Brusewitz, Chief Information Security Officer, at (562) 940-3873 or e-mail to abrusewitz@laccio.org.

JWF:AB:ygd

Attachment

c: Department Heads
Information Technology Managers
Information Systems Commission

P:\Final Documents\CIO\security\information security status_bdm.doc

Status of Information Security
County of Los Angeles
As of December 31, 2005

Jon W. Fullinwider
Chief Information Officer

Al Brusewitz, CISSP, CISM
Chief Information Security Officer

Table of Contents

Information Security Status for the County of Los Angeles 1
Introduction 1
Information Security Accomplishments 1
Security Organization 1
Information Security Steering Committee (ISSC) 2
Security Engineering Teams (SET) 2
Network Strengthening and Isolation (NSI) 3
Host Strengthening and Isolation (HSI) 3
Policy Development and Best Practices 3
CCERT 4
Antivirus Committee 4
Remote Access/Wireless Access (RAWA) 4
Network Controls and Protection Measures 4
Compliance and Privacy 6
Information Security Awareness 6
Additional Security Awareness Activities 6
Monitor and Audit 6
Physical Protection of Information Assets 7
Systems Implementation and Administration 7
Desktop and Laptop Systems 8
Los Angeles County Information Security Milestones and Accomplishments 8
Milestone/Accomplishments 8
Strategy 8
Business Automation Plan Security Survey Analysis 10
Security Manager/Department Information Security Officer (DISO) 10
Security Policy Compliance 10
Dial-Up Access 10
Information Security Awareness 11
Operating System Obsolescence 11
Antivirus and Patch Management 11
Information Security Expenditures 12
Summary 12

Information Security Status for the County of Los Angeles

Introduction

The Office of the Chief Information Officer (CIO) has taken aggressive actions to implement a countywide information security program over the past three years. Internet-based viruses and worms, along with the events of September 11, 2001 have heightened the awareness throughout the County that a strong centralized security approach is required to protect Los Angeles County information technology resources. Worldwide network connectivity has increased the risk to all organizations that utilize information technology and to the County. With the importance of information security measures being applied at all levels of the information technology infrastructure and organizations involved, the County must continue its efforts toward meeting the challenges and risks to IT assets. It is also important that the requirements be defined and included in organizational and countywide budgets to allow practical implementation.

The accomplishments and required activities for the County of Los Angeles are provided in this report to show a current status of the efforts of the Office of the CIO in meeting this challenge and plans for future improvements. All organizations in the county must participate in this ongoing effort for the good of the entire County since failure at any single point can allow an intruder to bypass the best security in place at all other departments.

Information Security Accomplishments

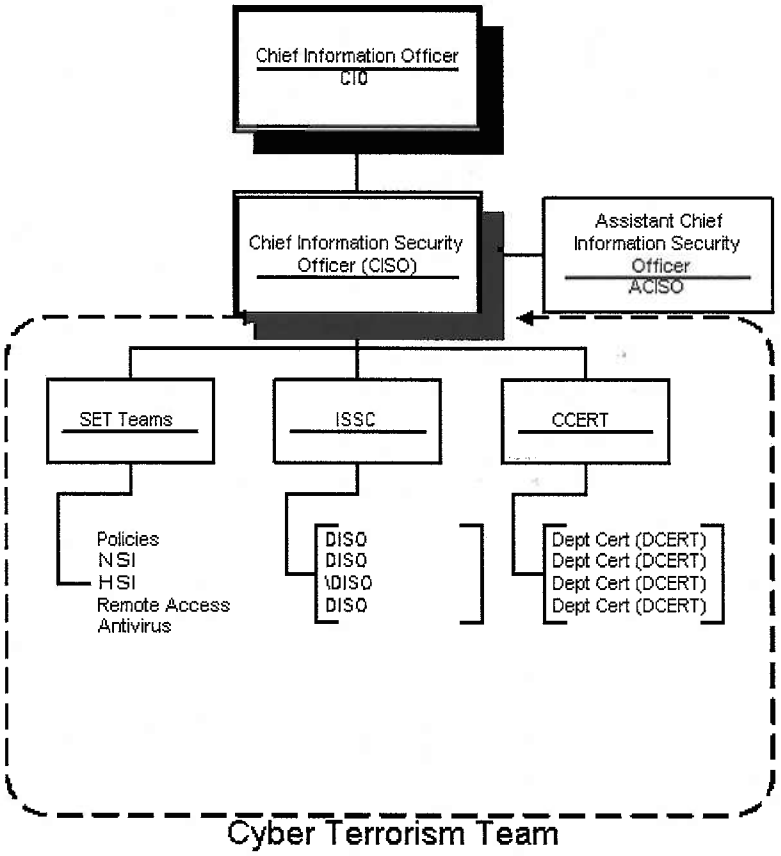
Security Organization

The CIO developed a security organization to ensure countywide implementation of the information security program within the County of Los Angeles. This process consisted of hiring a Chief Information Security Officer (CISO) in November of 2002, and appointment of an Assistant CISO (ACISO). Additionally, the CIO formed an advisory body called the Information Security Steering Committee (ISSC) with representation from each department in the form of appointed Department Information Security Officers (DISO). The CIO also instituted security engineering teams (SET) to develop standard approaches and select solutions for specific areas of information security. The County organizational efforts are almost complete as seen in the chart listed on Page 2 of this report.

However, each County department has IT assets that must be protected as well. Departments must take responsibility for their security programs by appointing responsible staff with information security responsibilities. Larger organizations will appoint full time DISOs along with required security support staff. Smaller departments cannot afford a full-time person for this purpose, but must assign information security

duties to existing staff and train them to participate in the County information security program. For those very small organizations, support must be provided from a central function such as the Internal Services Department (ISD).

Countywide Information Security Strategy Organization Chart



Information Security Steering Committee (ISSC)

The Information Security Steering Committee is composed of the Departmental Information Security Officers (DISO), the CISO and the Assistant CISO. This provides a forum for all information security-related collaboration and decision-making. Most of the departments have appointed DISOs and alternates to participate in ISSC activities and approve countywide policies, standards and guidelines.

Security Engineering Teams (SET)

Security Engineering Teams (SET) teams were established to address security from different access points and technologies. Teams are established and discontinued as needed depending on the issues that need to be addressed. The initial team appointments included Network Strengthening and Isolation (NSI), Host Strengthening and Isolation (HSI), Policies and Best Practices, Countywide Computer Emergency Response Team (CCERT), Antivirus, and Remote Access and Wireless Access (RAWA). In the last two

(2) years, additional SET assignments included Internet Content Filtering (ICF) and Anti-spam (AS) teams.

Network Strengthening and Isolation (NSI)

In its first year, the Network Strengthening and Isolation (NSI) team selected network intrusion detection systems (NIDS) to monitor network intrusions and forward messages to a system in the Network Control Center at ISD to display and monitor suspicious activities. These systems have been a tremendous success in blocking network attacks from worms and viruses as well as monitoring the health of the network and systems. They also selected host intrusion software that is currently being deployed on production servers and desktops to protect them from unauthorized activities.

The NSI team activities have been transferred to ISD Network Management to continue development of network protective measures and add to the NIDS deployment. This team is called the Network Security Task Force. The CISO and ACISO participate in these meetings to assist in addressing network security issues.

Host Strengthening and Isolation (HSI)

The Host Strengthening and Isolation (HIS) team has developed standard server implementation templates to support Windows 2000, Windows XP and is finalizing Windows 2003. In addition, they have developed a standard that applies to all servers scheduled for production implementation. The HSI team also researched and selected software to apply critical patches (PatchLink) and software to set up and maintain desktop systems (Altiris) that includes patching those systems. The systems have been acquired by several departments to manage their environments.

Policy Development and Best Practices

The Policy Development team completed and submitted policies that were approved by the Board and implemented for countywide use. These included:

- 6.100 Information Technology and Security Policy
- 6.101 Use of County Information Technology Resources
- 6.102 Countywide Antivirus Security Policy
- 6.103 Countywide Computer Security Threat Response
- 6.104 Use of Electronic Mail (e-mail) by County Employees
- 6.105 Internet Usage Policy
- 6.106 Physical Security
- 6.107 Information Technology Risk Assessment
- 6.108 Auditing and Compliance

The committee continues to work on additional policies and have submitted the following policy documents to the ISSC for review and approval.

- Information Technology and Disaster Recovery
- Information Technology Business Continuity
- Data Disposal
- Software Security
- Portable Devices/Storage Media Security
- Data Classification and Protection
- Security Training and Awareness
- Network Security (In Process)

CCERT

Response to information security events that affect several departments within the County must be coordinated and planned. The Countywide Computer Emergency Response Team (CCERT) was formed as a part of the Cyber Terrorism Task Force to provide the required coordinated response. The CCERT is comprised of membership from the various County departments and are often members of the Departmental Computer Emergency Response Team (DCERT). The CCERT team meets bi-weekly to review the latest threats and ensure that membership data is kept current. The CIO's office supports this effort and requires that the CISO participate in their activities, as well as lead the response to cyber events. The CCERT will continue its active role to coordinate DCERT development and to respond to incidents that occur.

Antivirus Committee

In 2001, the County selected Symantec and McAfee antivirus software as the standards for use on County IT systems and desktops. Departments were allowed to select one of these two systems depending on their preferences and ensure that the software was pushed out to the systems without end user intervention. The Antivirus Committee continues to meet on a biweekly basis to discuss ways to improve antivirus updates with the two County AV vendors. Recent events have caused them to explore the need and availability of software that controls spyware and its unwanted consequences that include tracking cookies, Trojan horses and keyboard monitoring.

Remote Access/Wireless Access (RAWA)

The Remote Access/Wireless Access (RAWA) team has produced a set of standards to support remote access policies and implement safeguards for them. They have also written a policy that calls for the elimination of modem dial up access within the County and submitted it to the policy committee for final review. The team has written and published a Wireless Security Guideline that is currently being utilized by ISD and others in wireless development security.

Network Controls and Protection Measures

The County has a large wide area network (WAN) with more than 70,000 devices connected and multiple external access points. Firewalls are in place to control access to and from the Internet, but that has not prevented massive infections by Internet based

worms that required weeks and multiple man hours to contain. Moreover, these infections caused untold losses in productivity within multiple departments because of the network traffic they generated and because the infected departments had to be isolated from the rest of the network until they could be disinfected.

In 2003, the CIO supported the acquisition of network intrusion detection and prevention measures (NIDS) designed to control unwanted penetrations into our networks. These systems included software and hardware that provided up-to-the-minute status to the ISD Network Control Center (NCC) based on activities of the NIDS, firewalls, and routers. This has allowed the NCC to conduct automatic blocking of offending systems or to manually isolate whole subnets where necessary to contain worms and viruses. In addition, departments were strongly encouraged to keep security patches and antivirus software current with push technology. As a result of these efforts, the County has not suffered a major outbreak of worms or viruses in the last 12 months, although there have been minor infections of e-mail based worms that were quickly contained.

Individual departments have suffered some infections because they failed to install critical patches that had been available for over a year. These departments now understand the need for rapid and current updates to anti-virus and operating systems.

Network protection efforts are continuing with the use of other software and hardware measures. In the past year, the CISO led a team to acquire and install spam control software throughout the County. The team selected Symantec's Brightmail. Licenses to support the various departments were justified and purchased through ITF funding for a three-year license that costs the County $270,000. Installation is complete for those departments that did not already have anti-spam protection in place.

Internet content filtering is a key initiative that was requested by the Board of Supervisors in 2003. A committee was established who selected a solution to be installed in the County at the Internet gateway. The software and hardware have been purchased at a cost of $420,000 and the system is in the process of being installed. Once completed, this system will prevent County Internet users from accessing sites that contain material deemed unacceptable for County use. When complete, the Internet Filtering Project will result in cost savings related to network usage and investigative resources that are required to stop misuse of County IT assets.

Additional projects have been initiated in the past year to protect instant messaging users from viruses and Internet risks and control the use of this tool on the County networks. Other software has been installed within ISD to test the ability to control the use of music and movie sharing programs that provide illegal access to copyrighted material. One of the most promising activities that is being supported by ISD is the Cisco Network Access Control (NAC) architecture. When fully implemented, the County will be able to enforce policies that mandate current anti-virus software, current patching and other controls. Any computer that attempts to connect to the County network from external or internal sources will be quarantined or rejected if security policy mandated updates are not present.

Compliance and Privacy

Privacy legislation is being implemented at the State and national levels that affects the County and the information in its systems. The Health Insurance Portability and Accountability Act (HIPAA) directly applies to the Department of Health Services, the Department of Mental Health and subsets of other departments mandating them to comply with its requirements for privacy of medical records. Other privacy legislation is in process at both the State and federal levels that also will support privacy requirements. The County is currently in the process of implementing procedures to comply with HIPAA, but the CIO is also committed to implementing measures that will make it compliant with future privacy legislation when enacted.

A major part of the HIPAA security rule compliance process was the requirement to perform a risk analysis for each of the covered components that included DHS, DMH, Probation Kirby Center and Sheriff's Pharmacy. An ITSSMA contract was executed with Fox Systems for $470,000 to perform that analysis. The analysis and reporting is complete. DHS requested additional technical analysis as an addendum to the contract that cost an additional $150,000 and that effort is also complete. Reports have been delivered to each of the covered components with a list of items that must be remediated. The covered components are in the process of developing project plans for those items that have not already been corrected. Final out briefing reports are in the process of being scheduled.

Information Security Awareness

The Employee Security Awareness Program will be developed and implemented through the use of automated learning management systems (LMS) as well as traditional classroom methods and published security reminders. It also will include training during employee orientation.

The CIO's office is participating in the project to acquire a LMS for County employee training. Once selected, information security training content will be acquired and implemented on the LMS to support the training program. This program will require a process for acquiring specific information security content that is tailored to Los Angeles County with specific requirements to operate on the County LMS.

Additional Security Awareness Activities

The Security website is near implementation and most of the content has been completed. New employee orientation material has been developed and submitted to Human Resources for presentation during the new employee orientation process. Other media methods such as pamphlets and electronic newsletters have been implemented as well. The basic part of awareness will be conducted through a web-based learning management system with specific security content developed to support County issues.

Monitor and Audit

A key information security activity that must be implemented throughout the County is monitoring and auditing of systems and applications. Network monitoring that is currently in place will be expanded to provide better coverage to provide early warning of

security events within the WAN and in the various departmental subnets. Automated monitoring of servers and applications must also be implemented to better support privacy requirements as well as provide forensic capabilities to determine unauthorized system access, who performed the action and what security risks have developed as a result of the incident. Countywide monitoring must be implemented to ensure that systems are properly implemented according to security standards. Departments must also implement audit processes that allow for the collection of activities as well as periodic reviews to determine if unusual events have occurred that might compromise security and integrity of the information involved.

Physical Protection of Information Assets

Computing assets receive the greatest amount of protection when kept in facilities that are designed to protect them environmentally, provide redundant support and have robust access control systems that record authorized entry and provide surveillance over activities that are conducted by the authorized personnel. All critical and sensitive systems should be contained in computing centers that are designed with protection in mind.

In the event that systems cannot be located in a central secure facility, the County will improve physical access controls over critical servers through improved systems and the implementation of automated access and recording systems. Use of employee identification badges must be enforced to control access to these critical assets.

Many systems for mail servers, standalone applications and PC-based systems are located in departmental facilities that are not well protected. In addition, telecommunications equipment is placed in areas that can be accessed by other departments as well as other non IT staff members. The County will be attempting to improve security over these systems in the coming year, and must continue to re-evaluate requirements as the systems grow and users become more dependent on them.

Systems Implementation and Administration

Computers that are installed in the County network must comply with standard baselines, be protected by antivirus software, be updated with all critical security patches and be maintained in accordance with the requirements that have been developed by the Host Strengthening Security Engineering Task Team. The standards are designed to provide common areas of security implementation as well as operating system-specific settings. Each computer must meet the standards that apply and scanned for vulnerabilities before being connected to the countywide area network (WAN) or departmental LAN. In addition, the system must be periodically scanned for vulnerabilities that may have been introduced over time.

System administration also must comply with policies and standards that have been developed to govern this process. Password controls, user account management and system updates must meet security standards that have been developed for that purpose. Continued efforts from the SET teams will be required to refine the standards and controls that apply.

User administrative procedures will be strengthened to ensure that only authorized users have access to the network and systems. Administrators will be required to audit user accounts on a monthly basis and suspend or delete any accounts that have not been used in the last 90 days. Additionally, actual employee data will be compared to the account files to ensure that only authorized users are granted access.

Desktop and Laptop Systems

Increasingly destructive worm attacks have demonstrated that personally assigned computers on desktops and mobile laptop devices are a threat to the County's networks due to their large numbers when infected. These attacks can create a denial of service situation when infected machines begin to emit large volumes of messages into the network. Because of this risk, a desktop strategy must be implemented that is designed to prevent worm and hacker attacks. The policies that have been implemented require that these systems be automatically updated with critical system patches as well as antivirus software. In addition, intrusion prevention software is being deployed to prevent day zero attacks where a signature of the malicious code has not been developed before the attack.

Los Angeles County Information Security Milestones and Accomplishments

Milestone/Accomplishments	Status	Date	Strategy
CISO/CIPO/ACISO	Complete	11/02	Security Management and Organization
Steering Committee	Complete	10/02	Security Management and Organization
Computer Emergency Response Teams	Complete	11/03	Security Management and Organization
Information Security Web Site	In progress	9/05	Sec Awareness
Standard Antivirus Contracts	Complete	3/02	Network Mgmt
Intrusion Detection Systems	Complete	4/04	Network Mgmt
Security Awareness Program	In Progress	7/30/06	User Security Awareness and Training
HIPPA Risk Analysis	Complete	10/15/05	Risk Mgmt
Secure Disposal Procedure	Future Objective	11/05	Physical
Standard Server Templates	W2K complete	11/18/04	System and net
Standard Server Templates	XP in process	1/05	System and net
Vulnerability Scans	Vendor Analysis	7/06	System and net

HIDS Implementation	In Process	6/20/06	System
Event Correlation (IDS)	Complete	2/04	System
Wireless Security Improvements	In Process	7/06	System
Implement HIPPA Security	In Process	5/06	Compliance and Privacy
County Vulnerability Assessment	Future Objective	1/06	Monitor and Audit
Wireless LAN Guidelines	Completed	3/13/2003	Policy, standards and procedures
Board Policy (Master Policy)	Completed	7/13/2004	Policy, standards and procedures
Internet Usage Security Policy	Completed	7/13/2004	Policy, standards and procedures
Use of County Information Technology Resources	Completed	7/13/2004	Policy, standards and procedures
Countywide Antivirus Security Policy	Completed	7/13/2004	Policy, standards and procedures
Use of Electronic Email by County Employees	Completed	7/13/2004	Policy, standards and procedures
Information Technology Risk Assessment	Completed	7/13/2004	Policy, standards and procedures
Auditing and Compliance Policy	Completed	7/13/2004	Policy, standards and procedures
Countywide Computer Security Threat Response	Completed	7/13/2004	Policy, standards and procedures
Physical Security	Completed	7/13/2004	Policy, standards and procedures
Information Technology Disaster Recovery	With ISSC	6/30/2005	Policy, standards and procedures
Information Technology Business Continuity	With ISSC	6/1/2005	Policy, standards and procedures
Data Disposal	With ISSC	6/1/2005	Policy, standards and procedures
Security Training and Awareness I	With ISSC	6/1/2005	Policy, standards and procedures
Software Security	With ISSC	6/1/2005	Policy, standards and procedures
Portable Devices/Storage Media Security	With ISSC	6/1/2005	Policy, standards and procedures
Data Classification and Protection	With ISSC	6/1/2005	Policy, standards and procedures
Incident Response	In Progress	6/1/2005	Policy, standards and procedures
Network Security	In Progress	6/1/2005	Policy, standards and procedures

Network Infrastructure Device Security	Completed	5/6/2003	Policy, standards and procedures
Minimum Standards for Configuring Antivirus Software for Windows Server	Completed	11/19/2003	Policy, standards and procedures
MS Windows 2000 Server Baseline Security Standards	Completed	11/19/2003	Policy, standards and procedures
MS Windows XP	With ISSC	6/30/2005	Policy, standards and procedures
MS Windows 2003	In Process	6/30/2005	Policy, standards and procedures
Patch Management Software Standard	Completed	9/25/2004	Policy, standards and procedures
CCERT Computer Security Threat Response	Completed	4/1/2003	Policy, standards and procedures

Business Automation Plan Security Survey Analysis

There were 37 responses to the 2005-2006 BAP security survey. The survey was designed to measure the security program status in the various departments and determine where CIO/CISO emphasis and assistance is required to strengthen the County information security program.

Security Manager/Department Information Security Officer (DISO)

Security managers or appointed department security officers (DISO) should be appointed to ensure that good security practices are implemented in the various departments. Of the total responses, 30 departments had a designated security manager/DISO and only 10 considered it a full-time duty. That number indicates that the larger departments could afford a full-time person for this purpose with the others supporting other tasks. Only seven (7) departments had no designated security manager/DISO on a full or part time basis.

Security Policy Compliance

The single most important part of the countywide information security program is to implement security policies that specify the Board's requirements for compliance. Most of the departments (36) indicated that they are compliant with the Information Security and Technology policies that were approved by the Board this year. The remaining department is assessing what is required to complete compliance.

Dial-Up Access

A major security goal for the CIO is to discontinue the use of remote dial-up to access servers in the county due to the security risk involved. Of the departments that stated they were aware of this strategy, two allowed remote dial-up access for the technical staff. All departments required VPN access and required two-factor authentications.

This is clearly an improvement in the security of remote access to County systems. Some study is required to determine if any of the remaining dial-up access is required to support applications; however, the majority must be eliminated and a policy is in development to support that goal.

Information Security Awareness

Information security awareness training is a key factor in developing an effective information security program. While the County is in the process of developing a countywide information security awareness program using a web-based system, it is important that each department consider their information security training needs and provide funding to support them. Of the 38 departments surveyed, 14 had requested information security awareness funding in their FY 05 – 06 budgets.

Operating System Obsolescence

Microsoft computer operating systems are subject to major upgrades almost every five years. Once issued, the current version of the operating system receives critical security patches as vulnerabilities are discovered. Microsoft discontinues issuing patches to servers and desktop devices at some point after the release of operating system upgrades, leaving those computers vulnerable to new viruses and worms that might infect them. Therefore, it is important that County departments replace operating systems that have become obsolete.

At the time of the survey, 14 departments noted that they had obsolete operating systems in their organizations. All of the departments that identified this problem have actively budgeted and implemented processes to replace those systems. Departments must begin to plan and budget replacement of the Windows 2000 operating system within the next two years to maintain operating system security within the County

Antivirus and Patch Management

The constant development of new viruses and discovery of operating system vulnerabilities require that computer systems throughout the County be maintained with the latest antivirus software and critical security patches. Failure in this area has been the single most significant security threat over the last few years.

The majority of departments indicated that they maintain current patches and antivirus software on their systems. Some departments have carried the process a step further and implemented software that maintains the entire system configuration in addition to providing patch management. They also indicated that they have automated the process and do not leave it up to users who would fail to stay current. Antivirus updates are also automated to ensure that the latest software is installed in a timely manner. This is a very important security success that has occurred in the last two years due to understanding the consequences of infections on the departments.

Information Security Expenditures

A common measure of security expenditures is to relate them to total information technology expenditures. The percentage for the previous two years is in line with industry standards that range from 2 to 4 percent. The CIO's office will continue to monitor security spending related to the total IT budget and will request refined numbers in upcoming budget plans.

.

Requirements	FY 2003 – 2004 Actual	FY 2004 – 2005 Actual
Total IT Budgets	**$ 564,091,674**	**$ 609,857,009**
Security Percent of IT	**4.4%**	**3.7%**
Security Budgets		
Staffing Costs *	$ 9,137,794	$12,280,482
Services and Supplies	$15,636,348	$ 9,672,544
Other Charges	$ 100,000	$ 10,019
Fixed Assets	$ 187,588	$ 516,980
Total	**$ 25,061,730**	**$ 22,480,025**

* Staffing costs are derived from salary and benefits for full time or percentages of employee activities used to support information security processes.

Summary

The County has made good progress in its security program and departments are actively participating in this effort. The Office of the CIO will continue to coordinate the program through the use of collaborative teams that include the Information Security Steering Committee (ISSC) and the various Security Engineering Teams (SET). An additional member of the CIO staff has been assigned to assist the Chief Information Security Officer (CISO) in this effort.

The information security program is not a one time process that can be accomplished with a few policies and technical tools. The nature of evolving threats to the County systems requires that the information security program be robust and continuous. Additional measures must be implemented in the coming years to improve security awareness, provide better monitoring and develop rapid computer incident response capabilities. Departments will continue to be asked to status their information security participation through the BAP security surveys, as well as participation in collaborative teams.

Appendix A – Security Survey Result

Information Security Survey

Question	AWM	Affrm Act	APD	Anm Cntl	Assesor	Aud Cntl	Bch & H
Is there a designated security Mgr/DISO	Yes	No	Yes	No	Yes	Yes	Yes
Compliant with Board security policies	Yes	Yes	Yes	No	Yes	Yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	No	N/A	N/A	N/A
If no, will you request a Board exemption	N/A	N/A	N/A	No	N/A	N/A	N/A
If no, did you request budget in 05/06	N/A	N/A	N/A	No	N/A	N/A	N/A
Will you be compliant in 2006	N/A	N/A	N/A	No	N/A	N/A	N/A
Remote dial-up access to servers allowed	No	No	No	No	No	No	No
Do you require remote access via VPN	No	Yes	N/A	Yes	Yes	Yes	Yes
Is antivirus software required for remote access	Yes	Yes	N/A	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	No	Yes	N/A	Yes	Yes	Yes	Yes
Did you include security awareness funding in your budget	No	No	No	No	No	Yes	No
Aware Microsoft announced non-support operating systems	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you have obsolete operating systems	No	No	No	Yes	No	No	No
If yes, do you have a plan to upgrade systems	N/A			Yes	Yes		Yes
Host intrusion on servers	No	No	No	No	Yes	No	No
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software updated automatically	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	No	Yes	No	Yes
Are security software patches current	No	Yes	Yes	No	Yes	Yes	Yes
Do you require signed acceptable use forms	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Departmental Security Rating							

Effective Security Practices
Improvements Required
Security is Deficient

Information Security Survey

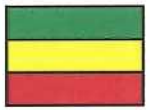
Question	BOS	CAO	CIO	CFS	Com Dev	CSS	CoSrSv
Is there a designated security Mgr/DISO	Yes	Yes	Yes	Yes	Yes	Yes	No
Compliant with Board security policies	Yes	Yes	Yes	Yes	Yes	Yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	N/A	N/A	N/A	N/A
If no, will you request a Board exemption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
If no, did you request budget in 05/06	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Will you be compliant in 2006	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Remote dial-up access to servers allowed	No	No	No	No	No	No	No
Do you require remote access via VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Did you include security awareness funding in your budget	Yes	No	Yes	No	No	No	No
Aware Microsoft announced non-support operating systems	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you have obsolete operating systems	No	No	No	Yes	No	No	No
If yes, do you have a plan to upgrade systems		No	Yes	Yes	N/A	N/A	N/A
Host intrusion on servers	No	No	No	No	No	No	No
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software updated automatically	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	No
Are security software patches current	Yes	Yes	Yes	Yes	Yes	Yes	No
Do you require signed acceptable use forms	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Departmental Security Rating							

Effective Security Practices
Improvements Required
Security is Deficient

Information Security Survey

Question	Cons Affr	Coroner	Counsel	DA	Fire	HR	DHS
Is there a designated security Mgr/DISO	No	Yes	Yes	No	No	Yes	Yes
Compliant with Board security policies	yes	Yes	Yes	Yes	Yes	Yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	N/A	N/A	N/A	N/A
If no, will you request a Board exemption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
If no, did you request budget in 05/06	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Will you be compliant in 2006	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Remote dial-up access to servers allowed	No	No	No	No	No	No	Yes
Do you require remote access via VPN	yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Did you include security awareness funding in your budget	No	No	Yes	Yes	No	Yes	Yes
Aware Microsoft announced non-support operating systems	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you have obsolete operating systems	No	No	No	Yes	Yes	No	Yes
If yes, do you have a plan to upgrade systems	N/A	N/A	N/A	Yes	Yes	N/A	Yes
Host intrusion on servers	No	No	No	No	No	No	No
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software updated automatically	Yes	Yes	yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are security software patches current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you require signed acceptable use forms	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Departmental Security Rating							

Effective Security Practices
Improvements Required
Security is Deficient



Information Security Survey

Question	HuRelcm	ISD	MH	Mil&Vet	Ombud	Park/Rec	Probat
Is there a designated security Mgr/DISO	Yes	Yes	Yes	No	Yes	Yes	Yes
Compliant with Board security policies	Yes	Yes	Yes	Yes	yes	yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	N/A	N/A	N/A	N/A
If no, will you request a Board exemption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
If no, did you request budget in 05/06	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Will you be compliant in 2006	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Remote dial-up access to servers allowed	No	No	No	No	No	No	No
Do you require remote access via VPN	Yes	Yes	Yes	No	Yes	Yes	Yes
Is antivirus software required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Did you include security awareness funding in your budget	No	Yes	Yes	Yes	No	No	No
Aware Microsoft announced non-support operating systems	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you have obsolete operating systems	No	Yes	No	No	No	Yes	Yes
If yes, do you have a plan to upgrade systems	N/A	Yes	N/A	N/A	N/A	N/A	N/A
Host intrusion on servers	N/A	Yes	No	N/A	No	No	No
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software updated automatically	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	No	Yes	Yes	Yes
Are security software patches current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you require signed acceptable use forms	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Departmental Security Rating							

Effective Security Practices
Improvements Required
Security is Deficient

Information Security Survey

Question	Pubdef	Pub Libr	Safety	PSS	PW	Reg Plan	Reg Rec
Is there a designated security Mgr/DISO	Yes	Yes	Yes	Yes	No	Yes	Yes
Compliant with Board security policies	Yes	Yes	Yes	Yes	Yes	Yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	N/A	N/A	N/A	N/A
If no, will you request a Board exemption	N/A	Yes	N/A	N/A	N/A	N/A	N/A
If no, did you request budget in 05/06	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Will you be compliant in 2006	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Remote dial-up access to servers allowed	No	No	No	No	Yes	No	No
Do you require remote access via VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	No	Yes	Yes	Yes	Yes	Yes
Did you include security awareness funding in your budget	Yes	No	Yes	No	No	Yes	Yes
Aware Microsoft announced non-support operating systems	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you have obsolete operating systems	Yes	Yes	No	Yes	No	No	Yes
If yes, do you have a plan to upgrade systems	Yes	Yes	Yes	Yes	N/A	N/A	Yes
Host intrusion on servers	No	No	No	Yes	No	No	No
Is antivirus software installed and current	Yes	No	Yes	Yes	Yes	Yes	Yes
Is antivirus software updated automatically	Yes	No	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are security software patches current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you require signed acceptable use forms	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Departmental Security Rating							

Effective Security Practices
Improvements Required
Security is Deficient

Information Security Survey

Question	Sheriff	TTC
Is there a designated security Mgr/DISO	Yes	Yes
Compliant with Board security policies	Yes	Yes
If not,do you have a compliance plan	N/A	N/A
If no, will you request a Board exemption	N/A	N/A
If no, did you request budget in 05/06	N/A	N/A
Will you be compliant in 2006	N/A	N/A
Remote dial-up access to servers allowed	No	No
Do you require remote access via VPN	Yes	Yes
Is antivirus software required for remote access	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes
Did you include security awareness funding in your budget	No	No
Aware Microsoft announced non-support operating systems	Yes	Yes
Do you have obsolete operating systems	Yes	No
If yes, do you have a plan to upgrade systems	Yes	N/A
Host intrusion on servers	No	No
Is antivirus software installed and current	Yes	Yes
Is antivirus software updated automatically	Yes	Yes
Is patch management software utilized	Yes	Yes
Are security software patches current	Yes	Yes
Do you require signed acceptable use forms	Yes	Yes
Departmental Security Rating		

Effective Security Practices
Improvements Required
Security is Deficient